

TEMA 1: ARQUITECTURA AVANZADA TCP/IP.

1. PROTOCOLO IPv6.

El protocolo de encaminamiento actual es IPv4, pero este protocolo está alcanzando el final de su vida útil. IPv4 presenta deficiencias que hace inadecuado su uso actualmente con los avances que ha tenido Internet, sobre todo a nivel multimedia.

IPv6 se diseña para solventar las deficiencias de IPv4 en la actual red Internet:

- 1. NUMERO DE DIRECCIONES IPv4 EN INTERNET SE VA CONSUMIENDO:** A pesar del uso de encaminamiento privado (subredes, superredes y NAPT), cuando se reclaman IP fijas publicas oficiales, puede provocar que las direcciones IP de terminen acabando.
La aparición de nuevos dispositivos TCP/IP especializados (dispositivos inalámbricos, teléfonos IP, receptores de televisión, electrodomésticos, etc) son los que demandan las direcciones IP publicas.
- 2. NO HAY DISTINCION ENTRE PAQUETES.** No existe en el diseño de IPv4 una codificación en la cabecera IP que distinga unos paquetes de otros (paquetes de audio)
IPv4 no ofrece prioridades diferenciadas para reducir el retardo de espera de un paquete en la cola del interfaz de salida de un router y descartar paquetes con menor prioridad en caso
Tampoco existe una identificación específica de flujos de paquetes para ofrecer una determinada calidad de servicio o recursos.
- 3. PERDIDA DE TIEMPO A LA HORA DE ENCAMINAR.** Debido al diseño de la cabecera IPv4 se pierde un tiempo extra en el encaminamiento de los datagramas en los routers.
La cabecera IPv4 es muy grande y se procesan demasiadas cosas en los routers, lo que hace el encaminamiento más lento.
- 4. NO TIENE IMPLEMENTADO NINGUN MECANISMO DE SEGURIDAD.** IPv4 no tiene implementado ningún mecanismo de seguridad en la cabecera, para aquellas aplicaciones que necesiten autenticación, cifrado e integridad de datos.

• CARACTERISTICAS DE IPv6:

IPv6 conserva lo mejor de IPv4, eliminando lo peor y añadiendo nuevas funcionalidades a través de cabeceras de información de control opcional.

IPv6 conserva las mismas características fundamentales que IPv4, el protocolo responsable del encaminamiento por Internet o por una red privada IP ofrece un servicio no orientado a conexión sin control de errores ni de flujo.

- **MAYOR ESPACIO DE DIRECCIONAMIENTO:** De 4 octetos a 16 octetos = 128 bits. Esto permite utilizar 2^{128} direcciones, es decir, incrementamos el factor de encaminamiento en 2^{92} .
- **SOPORTE PARA OFRECER PRIORIDAD Y CALIDAD DE SERVICIO:** Vamos a dar la misma calidad de servicio a todos los paquetes de una comunicación. Y se va a poder establecer retardos de espera en colas en los routers y descartes de paquetes con menor prioridad.
La cabecera IPv6 tiene unos campos específicos para establecer estas características.
- **MEJORAR EL RENDIMIENTO EN LOS ROUTERS:** Agilizar el proceso de encaminamiento, para ello se utiliza una cabecera fija de información de control más simple con la mitad de campos.
Se utiliza un nuevo formato flexible de cabeceras de extensión opcionales para utilizar servicios adicionales, como puede ser la fragmentación de paquetes, cuando se necesiten.
- **SOPORTE PARA OFRECER SEGURIDAD:** Se ofrece seguridad en la cabecera a través de cabeceras de extensión opcionales que se añaden a la cabecera fija.
Se implementa a través de la arquitectura IPsec para proporcionar cifrado, integridad y autenticación.

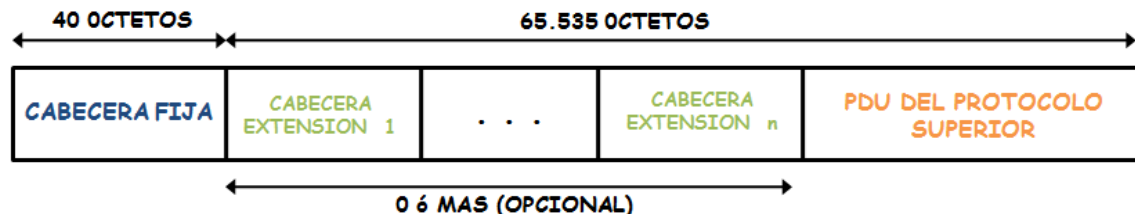
• SEGURIDAD:

El protocolo IPv6 tiene dos cabeceras de información de control opcionales que se corresponden con dos protocolos de la arquitectura IPsec.

En el protocolo IPv6 los protocolos IPsec están incluidos dentro del nivel IP.

El protocolo IPv4 usa los protocolos de la arquitectura IPsec pero en los niveles superiores al nivel IP.

1.1. DATAGRAMA IPv6.



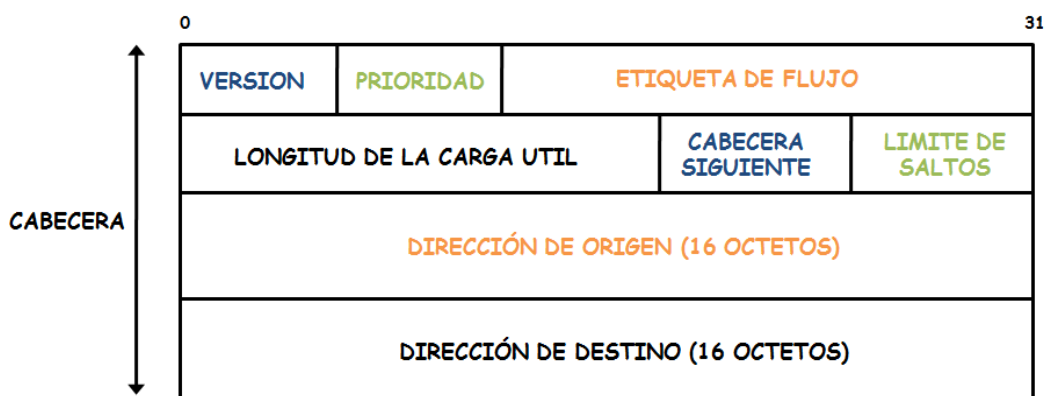
Vamos a tener una cabecera fija de información de control de 40 octetos y 0 o varias cabeceras opcionales y los datos del nivel superior (PDU).

• CABECERA FIJA:

Lleva información fundamental para el correcto encaminamiento de paquetes, mejorando el servicio ofrecido en IPv4.

Se elimina más de la mitad de los campos de la cabecera del paquete IP, con respecto al protocolo IPv4, para simplificar el diseño de los routers.

- FORMATO:



Algunos campos desaparecen:

- * El campo **OPCIONES** de IPv4 desaparece ya que se sustituye por las cabeceras opcionales de extensión. Mientras que en IPv4 los campos para la fragmentación son obligatorios en IPv6 los campos se incluyen dentro de una cabecera opcional, que solo se va a utilizar cuando sea necesaria la fragmentación de paquetes.
- * El campo **LONGITUD** desaparece porque la longitud de la cabecera de control es fija.
- * El campo **SUMA COMPROBACION** desaparece ya que no se comprueban errores físicos de la cabecera en el nivel IP, si se produjese algún error lo tendrá que detectar los niveles superiores.

Otros campos han sido renombrados:

- * **LONGITUD DE CARGA UTIL (16 bits):** (en IPv4 longitud total): son 65.535 octetos incluyendo las cabeceras opcionales más las PDU del nivel superior, es decir, excluyendo la cabecera fija.
- * **LIMITE DE SALTOS:** (en IPv4 TTL) Indica el numero de routers como máximo por los que un paquete puede ser encaminado.
- * **CABECERA SIGUIENTE (4 bits):** (en IPv4 Protocolo) Indica la siguiente cabecera, si es una cabecera de extensión o si el protocolo de la PDU del nivel superior.

Cuando el valor es conocido nos estaremos refiriendo a una PDU. Cuando el valor es desconocido vamos a suponer que hablamos de cabeceras de extensión.

* **PRIORIDAD (4 bits):** Prioriza el procesamiento de los paquetes dependiendo de la comunicación, minimizando el retardo en la interfaz de salida.

Cuando hay saturación, se va a priorizar de manera que el último paquete eliminado sea el más prioritario. Se define 16 niveles de prioridad de procesamiento para el paquete en función de si la aplicación está montada sobre TCP o UDP.

El nivel más prioritario es el nivel 15 y corresponde con el encaminamiento de paquetes de audio. Va montado sobre UDP.

* **ETIQUETA DE FLUJO (24 bits):** Ofrece calidad de servicio dependiendo del tipo de comunicación. Permite identificar los flujos para luego ofrecer a los paquetes de un flujo la misma calidad.

Un flujo es una secuencia ordenada de paquetes que siguen una misma ruta por internet desde un origen a un destino y que requieren de un tratamiento especial (recursos) en los routers por donde pasan.

* **DIRECCION DESTINO:** Es el campo más importante. Ya que siempre se va a encaminar a partir de esta dirección.

* **DIRECCION ORIGEN:** Fundamental para hacer encaminamiento ICMP.

Aunque la longitud es mayor que en IPv4 sin opciones el número de campos en IPv6 es casi la mitad. Una entidad IP intermedia encamina antes en IPv6 ya que se obvia la detección de errores físicos (que nunca se recuperan). Por tanto el datagrama va a procesarse más rápido y se va a agilizar el encaminamiento.

- MODELO DE SERVICIOS DIFERENCIADOS:

A pesar de los esfuerzos de estandarización, los campos de Prioridad y Etiqueta de flujo son campos de investigación y experimentación.

El modelo que se usa para ofrecer calidad de servicio es el modelo de Servicios Diferenciados (DiffServ).

DiffServ nace como un modelo más simple QoS. Utiliza una codificación de seis bits (DSCP) que se usa tanto en IPv4 como en IPV6.

* **DSCP:** Punto de Código de Servicios Diferenciados.

Está formado por seis bits que van a identificar el tipo de servicio.

El DSCP solo se aplica a los routers del dominio de un operador y lo pone el router de acceso. La calidad de servicio la ofrecen los operadores de comunicación pero hay que pagarla.

Para ofrecer la calidad de servicio usamos los 6 bits más significativos del campo TOS en IPv4 y en IPv6 se van a utilizar los 4 bits del campo prioridad y los dos más significativos del campo etiqueta de flujo.

El modelo de Servicios Diferenciados es el típico modelo para un grupo de routers que forman un dominio administrativo. La administración define un conjunto de clases de servicio con una determinada codificación DSCP.

Los datagramas IP del cliente que entran en un dominio contienen un campo de Tipo de Servicio solicitando una clase de servicio determinado y previamente contratado.

El router encamina por la dirección de destino del paquete, ofreciendo los recursos (buffers, ancho de banda, retardo de transmisión, etc....) indicados por la clase de servicio.

• CABECERA EXTENSION:

Son cabeceras opcionales que añaden nuevas funcionalidades que la cabecera fija no ofrece.

Pueden existir 0 ó N cabeceras de extensión, si hay más de una cabecera de extensión deberemos poner todas las cabeceras que necesitemos.

Todas la cabeceras tienen una determinada secuencia y un id que las identifica, es decir, las cabeceras de extensión tienen un orden determinado. Cabecera siguiente va a indicar el id de la siguiente cabecera de extensión.

CABECERA FIJA SIGUIENTE=0	CABECERA SALTO A SALTO SIGUIENTE = 43	CABECERA DE ENCAMINAMIENTO SIGUIENTE = 44	CABECERA FRAGMENTACION SIGUIENTE = 51	CABECERA AUTENTICACION SIGUIENTE = 6	SEGMENTO TCP
-------------------------------------	---	---	---	--	---------------------

CODIGO DE LA CABECERA	TIPO DE CABECERA
0	Salto a salto
43	Encaminamiento
44	Fragmentación
51	Autenticación
50	Encapsulado de seguridad de la carga útil
60	Opciones para el destino
.....

Cuando no hay cabeceras de extensión, cabecera siguiente va a indicar el protocolo de la PDU



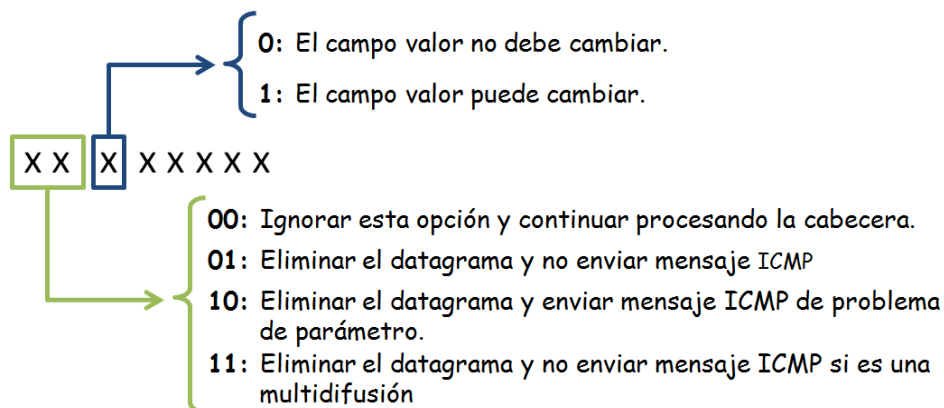
CODIGO DE PROTOCOLO	TIPO DE PROTOCOLO
6	TCP
17	UDP
1	ICMP
4	IP

- TIPOS DE CABECERAS DE EXTENSION:

* **CABECERA DE OPCIONES SALTO A SALTO:** Proporcionan información especial para los routers en cada salto. Tiene dos opciones principales: Jumbograma (cuando el paquete ocupa más de 65.536 octetos de información) y alerta al router.



- **LONGITUD DE CABECERA:** Indica el número de opciones que aparecen a continuación, en bloques de al menos 8 octetos.
- **TIPO:** Indica la opción. Si el destino no se sabe qué hacer con la opción se observa los dos primeros bits:



- **LONGITUD:** Indica la longitud en octetos del campo valor.

* **JUMBOGRAMA:** Se diseñaron para enviar datagramas de gran tamaño. Se usan en aplicaciones de

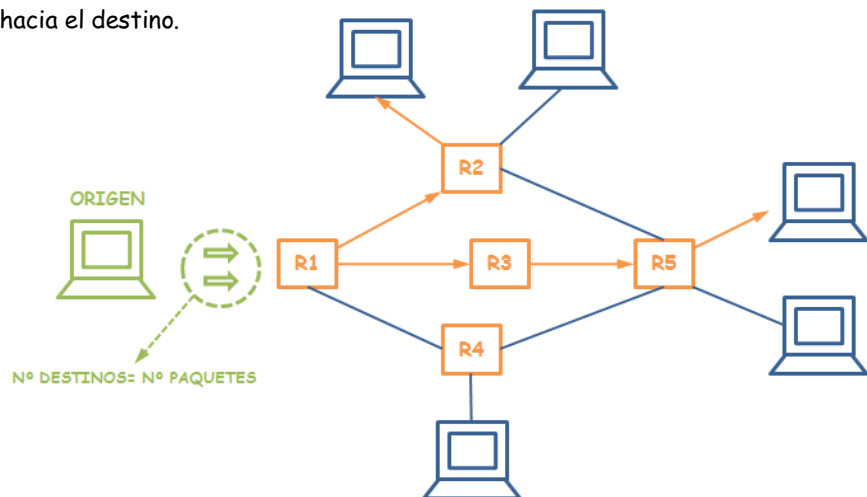
- * **CABECERA DE AUTENTICACION:** Permite la verificación de la autenticidad del emisor y la integridad del contenido del paquete.
- * **CABECERA DE ENCAPSULADO DE SEGURIDAD DE LA CARGA UTIL:** Proporciona información sobre los tipos de mecanismos de seguridad utilizados para garantizar los servicios de confidencialidad del contenido del paquete. Dispone de la opción de autenticación e integridad, lo que nos permite no usar la cabecera de Autenticación.
- * **CABECERA DE OPCIONES PARA EL DESTINO:** Lleva información opcional que debe ser procesada por el destino final del datagrama. Tiene el mismo formato que la cabecera de opciones salto a salto.
- * **CABECERA DE MOVILIDAD:** IP móvil v6. Es una cabecera específica.

1.2. TIPOS DE DIRECCIONES EN IPv6.

- **UNIDIFUSION (UNICAST):** Transmisión punto a punto (comunicación 1 a 1) desde un sistema final origen a un sistema final destinatario.

Por cada paquete IP que envías lo tienes que replicar por el número de destinos a los que van dirigidos. Si hay n destinatarios hay que transmitir n copias de la misma información.

Simplifica el encaminamiento, dices a donde quieres que vaya cada paquete (cada equipo tiene su propia IP) y los routers se encargan de encaminar hacia el destino.

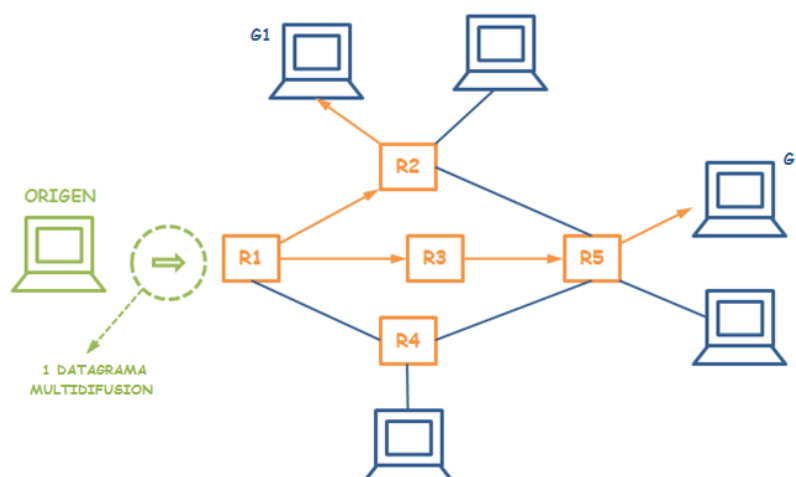


- **PROBLEMA:** Se está replicando la información de forma innecesaria cuando lo único que cambia es la IP destino. Proceso de envío independiente desde una máquina origen a una única máquina destino. Algunos enlaces deben transportar varias copias.

- **MULTIDIFUSION:** Transmisión en un solo envío, desde un sistema final origen a todos los sistemas destinatarios de un grupo de multidifusión que comparten una misma dirección IP de multidifusión correspondiente al grupo.

Además de su IP cada equipo puede asimilar otras direcciones IP para conectar vía multicast.

La comunicación es 1 a n con entrega a n interfaces, pero la información solo se transmite una vez desde el sistema origen.



Desde la maquina origen solo sale un único paquete IP, son los routers los que lo copian para encaminar a los distintos equipos con mismo grupo multicast.

Los routers de multidifusión por Internet manejan direcciones IP de multidifusión.

Multidifusión consiste en un único proceso de envío independientemente del número de maquinas receptoras de una misma información desde una maquina origen a todas las maquinas destinatarias que pertenecen al mismo grupo de multidifusión.

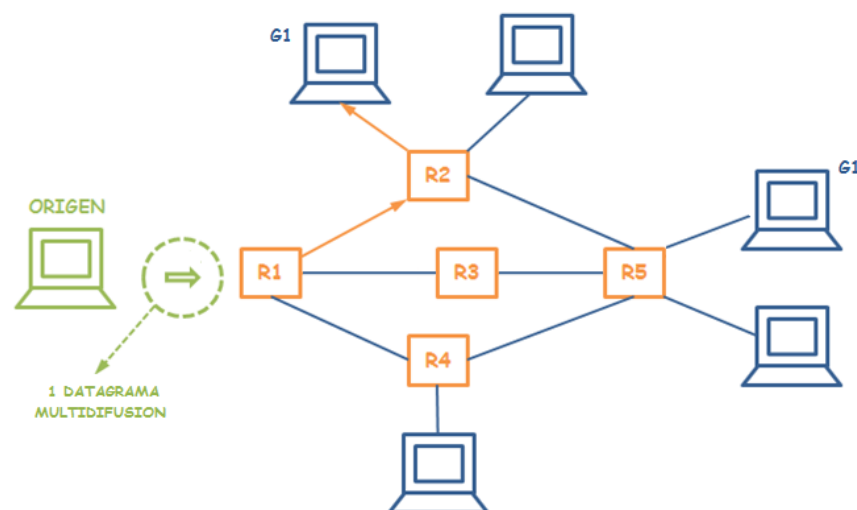
Cada enlace transporta una única copia.



- **DIFUSION (BROADCAST):** Es un caso particular de de multidifusión. Transmisión, en un solo envío, desde un sistema final origen a todos los sistemas conectados a una misma red de área local de difusión
Consideramos una red de área local como un grupo de multidifusión.

- **MONODIFUSION (ANYCAST):** Es como multicast pero solo se envía el datagrama al interfaz más cercano del grupo de monodifusión.

Transmisión, en un solo envío, desde un sistema final origen al sistema destinatario más cercano de un grupo de monodifusión que comparte una misma dirección de monodifusión.



La comunicación es 1 a n con entrega a n interfaces.

Envío a una (cualquiera) de las interfaces indicadas que, generalmente, es la más cercana.

El sistema origen debe utilizar un protocolo basado en una métrica de distancias para encontrar al sistema más cercano.

Monodifusión consiste en un único proceso de envío independiente del numero de maquinas receptoras de una misma información desde una maquina origen a una única maquina destinataria (la más cercana) que pertenece a un grupo de monodifusión que comparten una misma dirección de monodifusión.

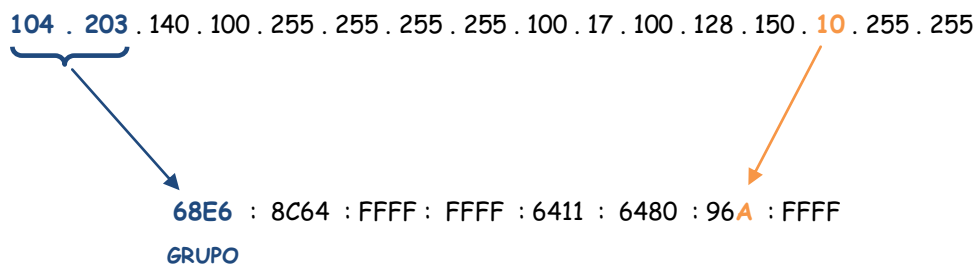
1.3. SINTAXIS DE DIRECCIONAMIENTO IPv6.

Una dirección IPv6 son 16 octetos en decimal. Para simplificar el formato vamos a usar 8 grupos de cuatro dígitos hexadecimales de dos octetos en decimal cada uno.

1 DIR IPv6 = 16 OCTETOS DECIMALES = 8 GRUPOS DE 4 DIGITOS HEXADECIMALES.

2 OCTETOS DECIMAL = 1 GRUPO DE 4 DIGITOS HEXADECIMAL

Los grupos se separan por dos puntos ":" y están escritos en hexadecimal.



Los ceros a la izquierda de un grupo pueden omitirse.

Uno o más grupos consecutivos de ceros se pueden sustituirse por una pareja de dos puntos "::". Solo se puede usar una pareja de dos puntos.

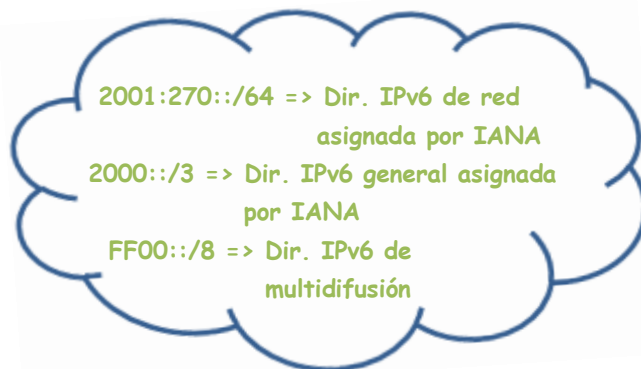
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 = 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 = :: 1

Usa la notación de superred o CIDR: DIR IPv6 /LONGITUD PREFIJO.

• **PREFIJO:** Las direcciones en IPv6 tienen prefijos en vez de las mascarar que se usan en IPv4.

La longitud del prefijo indica un conjunto mínimo de bits comunes del PREFIJO que no se deben cambiar y que identifican unívocamente a cualquier clase de la DIRECCION IPv6.

En las redes IPv6 el prefijo es siempre /64, es decir, las redes en IPv6 son de tamaño fijo.



- EJEMPLO:

2100 : 720 : 0000 : 0000 : 0CD3 : 00A3 : 34DF : 2132 /64 => 2100 : 720 : 0 : 0 : CD3 : A3 : 34DF : 2132 /64 =>

2100 : 720 :: CD3 : A3 : 34DF : 2132 /64

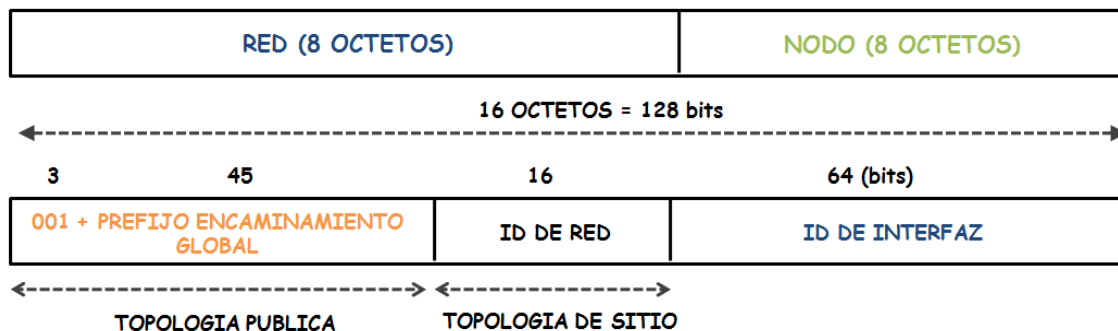
• **FORMATO URL:** En una URL los dos puntos indican opcionalmente el número de puerto.

La dirección IPv6 debe ir contenida entre corchetes (p.ej, [http:// \[2001:720::212:6BFF:FE11:1111\] : 80/index.html](http://[2001:720::212:6BFF:FE11:1111]:80/index.html))

1.4. DIRECCIONES IPv6 DE UNIDIFUSION.

En función del ámbito o contexto podemos distinguir dos tipos de direcciones IPv6: Globales y Locales. Además se pueden distinguir direcciones especiales de transición, especiales de bucle (loopback) y especiales no específicas.

- **DIRECCIONES GLOBALES:** Transmisión punto a punto (comunicación 1 a 1) desde un sistema final origen a un sistema final destinatario.



* **NODO = ID DE INTERFAZ:** Indica la maquina dentro de la red.

* **TOPOLOGIA PUBLICA (48 bits) = PREFIJO DE SITIO (ORGANIZACIÓN):** Está formado por prefijo IANA (001), el registro regional, el ISP y el sitio.

El prefijo IANA (001) lo asigna la IANA-ICANN. Las direcciones IANA son de la forma 2000::/3 (estándar).

* **TOPOLOGIA DE SITIO:** Asignado por el administrador de la organización.

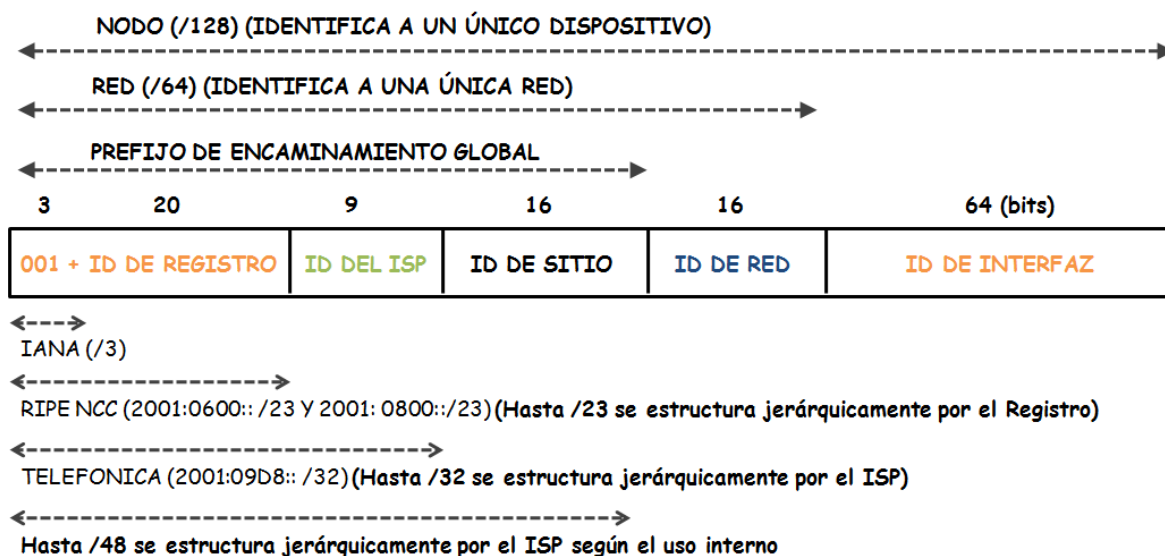
Puede crear 65.536 subredes o múltiples niveles jerárquicos de direcciones y una eficiente infraestructura de encaminamiento.

Con un prefijo /48, cada organización obtiene 2^{16} redes de hasta 2^{64} dispositivos cada una.

Como se puede ver la red siempre va a tener prefijo /64.

- **OBTENCION DEL PREFIJO:** El prefijo de encaminamiento global es un valor asignado a una organización (sitio), es decir, a un conjunto de redes o enlaces.

El prefijo se ha diseñado para ser estructurado jerárquicamente por los Registros y los ISP.



IANA asigna un identificador único al Registro Regional. El Registro Regional asigna un identificador único al ISP (operador)

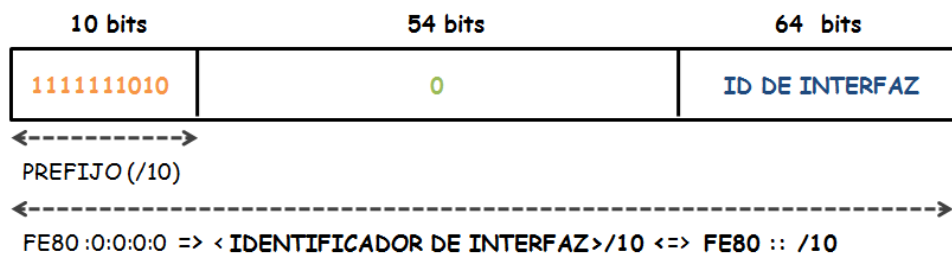
El ISP asigna un identificador único al Sitio (organización o usuario final), el administrador del Sitio asigna un identificador único a las redes y maquinas.

• **DIRECCIONES LOCALES AL ENLACE:** Permiten comunicar nodos dentro de un mismo enlace físico (nivel de enlace)

No pueden ser encaminadas al exterior.

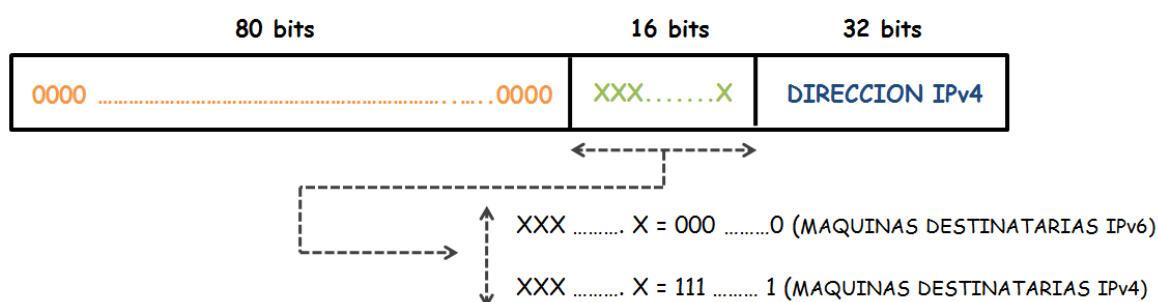
No interviene ningún router (enlace aislado con el exterior).

Útiles en redes sin routers.



• **DIRECCIONES ESPECIALES DE TRANSICION:** Son direcciones de transición de IPv4 a IPv6 ya que la mayoría de los routers son IPv4

Hay dos tipos de direcciones especiales de transición, las compatibles con IPv4 y las mapeadas a IPv4:



- **COMPATIBLES IPv4 (::IPv4/128):** Para túneles automáticos sobre IPv4.

Las maquinas destinatarias son IPv6 (p.ej, :: 138.10.9.16).

- **MAPEADOS A IPv4 (::FFFF: IPv4 /128):** Para comunicar terminales con doble pila y utilizando direccionamiento IPv6 sobre redes IPv4.

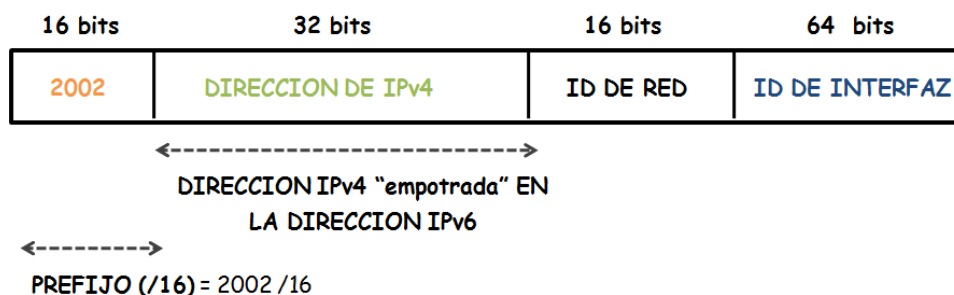
Se usa para enviar tráfico desde un terminal IPv6 tráfico a un terminal IPv4.

Las maquinas destinatarias son IPv4 (p.ej, ::FFFF: 138.10.9.16).

Hay otro tipo de direcciones de transición, las de Estrategia 6to4:

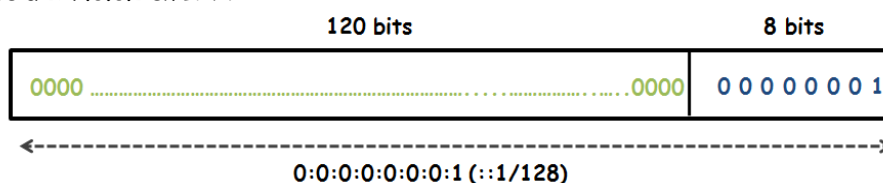
- **ESTRATEGIA 6to4 (2002:IPv4::/16):** Para túneles automáticos sobre IPv4

La dirección IPv4 está en hexadecimal. (p.ej, 129.146.86.187 = 8192:56BB)



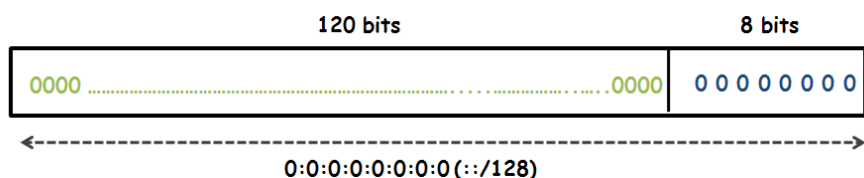
• **DIRECCIONES ESPECIALES DE BUCLE (loopback):** Se utiliza para autoenvío de paquetes

Equivalente a 127.0.0.1 en IPv4



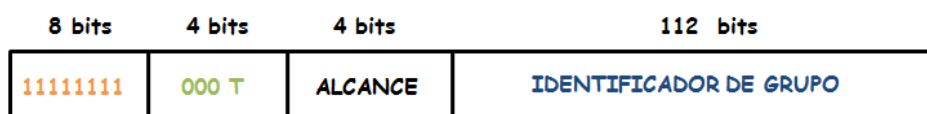
- **DIRECCIONES ESPECIALES DIR NO ESPECÍFICA:** Se utiliza temporalmente cuando no se ha asignado ninguna dirección.

Se utilizan en autoconfiguración de direcciones



1.5. OTRAS DIRECCIONES IPv6.

- **DIRECCIONES MULTIDIFUSION (FF00::/8):** Solo pueden usarse como direcciones de destino y nunca como direcciones de origen.



* T (TRANSITORIO):

- T=0: Dirección no transitoria o asignada permanentemente por IANA/ICANN.
- T=1: Dirección transitoria o no asignada permanentemente.

* ALCANCE o AMBITO: Limite del grupo de multidifusión. Numero entero de 4 bits.

- ALCANCE =0 y ALCANCE =F: Reservado.
- ALCANCE =1: Nodo local o en la propia maquina.
- ALCANCE =2: Enlace local
- ALCANCE =5: Sitio local (varios enlaces)
- ALCANCE =8: Organización local (compuestas de varios sitios o centros)
- ALCANCE =E: Alcance Global ("en Internet")

* IDENTIFICADOR DE GRUPO: Identifica el grupo de multidifusión permanente o temporal dentro de un determinado alcance o ámbito.

- **EJEMPLO:** Si asignamos una dirección permanente al Grupo de servidores en tiempo (NTP) = 101.

- FF01::101 => Todos los NTP en el mismo nodo que el paquete origen.
- FF02::101 => Todos los NTP en el mismo enlace que el paquete origen.
- FF05::101 => Todos los NTP en el mismo sitio que el paquete origen.
- FFOE::101 => Todos los NTP en Internet.

- **DIRECCIONES MONODIFUSION:** No tienen un espacio propio dentro del direccionamiento IPv6 (utilizan el mismo espacio que las de unidifusión).



No se puede distinguir entre direcciones de unidifusión y monodifusión ya que pueden existir direcciones de unidifusión de ámbito local o global

Solo se pueden usar como direcciones de destino nunca como direcciones de origen.

1.6. CONFIGURACION DE DIRECCIONES IPv6.

Además de la configuración manual, podemos diferenciar dos modos de configuración de una dirección IPv6, configuración predeterminada o configuración automática.

- **DHCPv6 ("Stateful" o predeterminada):** Es similar a DHCPv4.

Ofrece configuración dinámica y fija de direcciones IP junto con el resto de información TCP/IP (router siguiente, servidores DNS, etc ...)

- **AUTOCONFIGURACION ("Stateless" o automática):** Usa el protocolo ND (Neighbor Discovery)

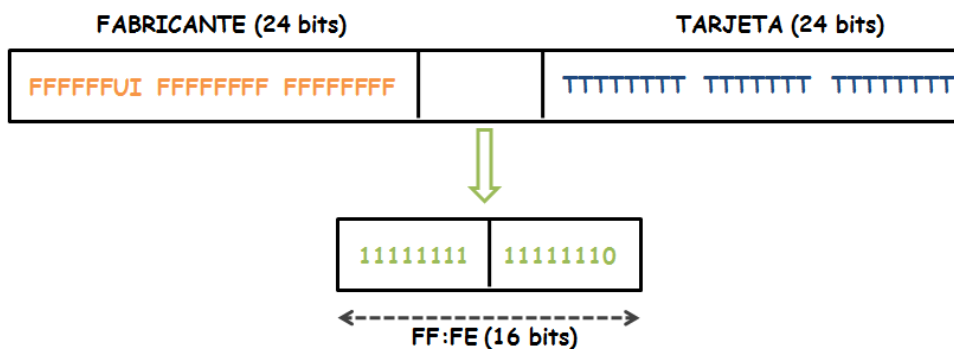
No requiere ninguna configuración previa del sistema ni servidores adicionales.

Un router anuncia el prefijo de red (8 octetos) que debe utilizarse en el enlace.

Los nodos generan un identificador de dispositivo (8 octetos). Esto se puede hacer de manera pseudoaleatoria o basándose en la dirección física o IEEE 802 MAC obtener la EUI-64.

- **OBTENER ID. DE INTERFAZ EN EUI-64 PARA UNA DIR DE UNIDIFUSION:** IEEE define el formato de dirección EUI-64 de 64 bits para obtener el identificador de Interfaz (nodo o sistema o dispositivo) a partir de una dirección IEEE 802 MAC de 48 bits (6 grupos de 2 dígitos hexadecimales)

El Identificador de Interfaz se construye, generalmente, según el formato EUI-64:



- * **IDENTIFICADOR DE FABRICANTE = 24 bits.**

Se pone a 1 el bit U/L para indicar alcance universal. Si lo pusiéramos a 0 indicaríamos que el alcance es local.

Se pone a 0 el bit I/G para indicar que es una dirección de unidifusión (Individual). Si lo pusiéramos a 1 indicaríamos multidifusión (Grupo).

- * **IDENTIFICADOR (Nº SERIE) DE LA TARJETA = 24 bits**

- * **FF:FE:** Se inserta en el centro de la dirección IEEE MAC-48.

- **CONVERSION DE 802 MAC A EUI-64:**

DIR MAC = 6 OCTETOS (48 bits) = 6 GRUPOS DE 2 DIGITOS HEXADECIMALES
DE 1 OCTETO CADA GRUPO

ID DE INTERFAZ EN EUI-64 EN UNA DIR IPv6 DE UNIDIFUSION = 8 OCTETOS (64 bits) =
8 GRUPOS DE 4 DIGITOS HEXADECIMALES DE 2 OCTETOS CADA GRUPO

00:00:0B:0A:2D:51 => 0200:0BFF: FE0A: 2D51
00:AA:00:3F:2A:1C => 02AA:00FF: FE3F: 2A1C } → (0 => 001(U)0(I) => 2)

2. PROTOCOLO ICMPv6.

Es un protocolo de envío de mensajes de control (errores e información) en Internet. El destino del mensaje ICMP será el origen del datagrama IP.

El protocolo ICMP esta tan íntimamente ligado al protocolo IP que de hecho se puede ver como un protocolo más dentro del propio protocolo IP.

Usa la misma estrategia y tiene los mismos objetivos que la versión 4. Algunos protocolos independientes (ARP e IGMP) en IPv4 son parte de los mensajes ICMPv6.

1. **PROTOCOLO ND (Neighbor Discovery):** Protocolo de descubrimiento de vecino. Sustituye al protocolo ARP añadiendo más funcionalidades mediante mensajes ICMPv6.
2. **PROTOCOLO MLD (Multicast Listener Discovery):** Equivalente al protocolo IGMP de IPv4 . Utiliza mensajes ICMPv6 para gestionar la pertenencia a grupos multidifusión.

2.1. TIPOS DE MENSAJES ICMPv6.

• **MENSAJES ICMPv6 DE ERROR:** Tipo: 0 .. 127

- DESTINO INALCANZABLE:

0	8	16	31
TIPO = 1		CODIGO = 0-4	CHECKSUM
NO UTILIZADO = 0			
Copia de la máxima cantidad de datos del datagrama originario del error sin exceder tamaño máximo de la MTU			

1. Código: Indica el tipo de error por el cual no se ha realizado el envío correctamente. Toma valores de 0 a 4

- * 0: Sin ruta al destino
- * 1: La comunicación con el destino está prohibida por el administrador
- * 2: Sin vecino
- * 3: Protocolo inalcanzable
- * 4: Puerto inalcanzable

Este tipo de mensajes pueden llegar a ser idénticos tanto en IPv6 y en IPv4

- PAQUETE DEMASIADO GRANDE:

0	8	16	31
TIPO = 2		CODIGO = 0	CHECKSUM
MTU			
Copia de la máxima cantidad de datos del datagrama originario del error sin exceder tamaño máximo de la MTU			

Los routers IPv6 NUNCA fragmentan, en este caso el encargado de ensamblar va a ser la maquina destino como en IPv4, pero en IPv6 el único que fragmenta es la maquina origen.

Con este mensaje se le indica a la maquina origen que reduzca el tamaño del paquete conforme a las necesidades del destino.

- TIEMPO EXCEDIDO:

0	8	16	31
TIPO = 3	CODIGO = 0 ó 1	CHECKSUM	
NO UTILIZADO = 0			
Copia de la máxima cantidad de datos del datagrama originario del error sin exceder tamaño máximo de la MTU			

1. Código: Indica el tipo de error por el cual no se ha realizado el envío correctamente. Toma dos posibles valores 0 ó 1

- * 0: Limite de saltos en tránsito excedido
- * 1: Tiempo de reensamblado excedido

- PROBLEMAS CON LOS PARAMETROS:

0	8	16	31
TIPO = 4	CODIGO = 0-2	CHECKSUM	
PUNTERO			
Copia de la máxima cantidad de datos del datagrama originario del error sin exceder tamaño máximo de la MTU			

1. Código: Indica el tipo de error por el cual no se ha realizado el envío correctamente. Toma valores de 0 a 2

- * 0: Se ha encontrado un campo erróneo en la cabeza
- * 1: No se reconoce el tipo de cabecera siguiente
- * 2: No se reconoce la opción IPv6

• MENSAJES ICMPv6 DE INFORMACION: Tipo: 128 .. 255

- SOLICITUD Y RESPUESTA DE ECO:

0	8	16	31
TIPO = 128 ó 129		CODIGO = 0	CHECKSUM
IDENTIFICADOR		NUM SECUENCIA	
Datos opcionales de longitud arbitraria			

- * Tipo: Indica si el mensaje es de solicitud (Tipo= 128) o de respuesta (Tipo=129)